UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE.
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/729,943	12/09/2003	William E. Freeman	149391	2711

38598 7590 07/06/2007

ANDREWS KURTH LLP
1350 I STREET, N.W.
SUITE 1100
WASHINGTON, DC 20005

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
07/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/729,943	FREEMAN ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-27 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-27 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 have been examined.

Claim Objections

2. Claim 24 is objected to because of the following informalities: "to be replaces" (line 3) should be changed to "to be replaced". Appropriate correction is required.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 1-15 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-15 are directed to a protocol which does not fall within one of the four statutory classes of § 101. Applicant is suggested to change the claimed subject matter from a protocol to a method. For prior-art rejection purposes, the claims are treated as method claims.

5. Claims 16-20 are rejected under 35 U.S.C. 101. The claimed inventions are directed to a method for secure replacement of private keys;

however, the claimed method is not complete because the claims do not recite any step(s) for replacing the private keys. Since the claimed method does not achieve its intended purpose, it does not have a practical application and are non-statutory.

6. Claims 21-27 are rejected under 35 U.S.C. 101 because the claims are directed to non-statutory subject matter. Regarding claim 21, it is not tangibly embodied as it is only software per se. For an apparatus or a machine to be a physical object, at least one recited element must be hardware. Since all elements of the claim can be reasonably interpreted in light of the disclosure by one of ordinary skill as software alone (page 8, lines 20-22), the claim is directed to software *per se* and is non-statutory.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claim 6 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 6 recites the limitation "deleting the SKRP key". The SKRP key is the new/updated key. It is not clear why the method for key replacement deletes the new/updated

key. For prior-art rejection purpose, the limitation is interpreted as "deleting the identified private key".

9. Claim 10 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 10 recites the limitation "comparing the read key identifier to key identifiers of previously deleted private keys" (lines 4-5). It is not clear how identifiers of keys can be used if keys have been deleted.

10. Claims 16-20 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: replacing the one or more private key and singing the challenge with the SKRP keys (fig. 7, steps 560-570).

11. Claim 24 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: reject the SKR request if the identity of the private key to be replaced matches any of

the identities of the previously deleted private keys. This step is used to detect replay attack.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 1-6, 14-16, 18-21 and 25-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asanoma et al. (2003/0056099) in view of Chen et al. (7,099,476). Asanoma discloses a method and apparatus for updating a private key in a smart card containing multiple private keys (Abstract; figure 5). Chen discloses a method for updating a ciphering key including the steps for verifying that a correct key has been updated (Abstract; fig. 2, steps 220-250).

Regarding claims 1-6, 16, 18-21 and 25-26, Asanoma discloses a method and apparatus for secure replacement of a private key in a smart card containing multiple private keys, comprising: receiving a rekey request including an encrypted replacement private key (fig. 7, step 22); authenticating the rekey request (i.e., decrypting the encrypted replacement

private key using a key shared with a central system) (fig. 7, step 25); replacing the private key with the replacement private key (fig. 7, step 25). Asanoma does not explicitly disclose that the rekey request identifies a private key for replacement; however, this feature is deemed to be inherent to Asanoma method because figures 5 and 9 show that the smart card stores multiple private keys. The smart card would not know which key among the stored private keys to be updated if the request did not include the identifier of the key to be updated.

Asanoma does not discloses sending a challenge to the smart card where a key is to be updated, encrypting the challenge with the new/updated key, and returning the encrypted challenge. Chen discloses a method for updating a ciphering key at a node including sending a challenge to the node where a key is to be updated, encrypting the challenge with the new/updated key, and returning the encrypted challenge (fig. 2, steps 220-250). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Asanoma's method to include the steps of sending a challenge to the smart card where a private key is to be updated, encrypting the challenge with the updated private key, and returning the encrypted challenge, as taught by Chen. The motivation for doing so would have been to confirm that a correct key has been updated (col. 6, lines 46-49).

Regarding claims 14-15, Asanoma does not disclose that the private key is used to access a document, to perform on-line banking/purchasing or to view a web site content. Official Notice is taken that both concept and advantage of using public key infrastructure (PKI) in different fields including content access and/or on-line transactions are well known and expected in the art. It would have been obvious to use the private key in different fields including content access and/or on-line transactions as the PKI is known for providing better security and easier key management.

14. Claims 7-8, 17, 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asanoma and Chen as applied to claims 1, 16 and 21 above, and further in view of Shambroom (6,198,824). Asanoma does not disclose that the rekey request includes a time stamp. Shambroom discloses including a timestamp in a message to restrict replay attacks (col. 8, lines 4-10). It would have been obvious to modify the combined method of Asanoma and Chen to include a time stamp in the rekey request, as taught by Shambroom, in order to restrict replay attack (col. 8, lines 4-10).

15. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Asanoma, Chen and Shambroom as applied to claim 8 above, and further in view of Morimoto (7,024,553). Asanoma, Chen and Shambroom do not

disclose a time limit for rekeying. Morimoto discloses a method for updating encryption keys wherein the time limit for rekeying is one day or more depending on system requirements. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Asanoma, Chen and Shambroom to set the time limit for rekeying to one day or more, as taught by Morimoto, in order to meet the system requirements.

16. Claims 11-12 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asanoma and Chen as applied to claims 1 and 25 above, and further in view of Appenzeller et al. (6,886,096). Asanoma discloses receiving the rekey request from a key generator (fig. 3, element 11) which is separate from a certificate authority (fig. 3, element 22). Appenzeller discloses that a key generator and a certificate authority can be combined into one entity (col. 21, lines 18-24). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Asanoma and Chen to combine the key generator and the certificate authority into one entity, as taught by Appenzeller. The motivation for doing so would have been to reduce network traffic communicated between them.

17. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Asanoma and Chen as applied to claim 1 above, and further in view of Menezes et al. ("Handbook of Applied Cryptography"). Asanoma does not disclose signing the rekey request and verifying the corresponding signature. Menezes discloses signing a message containing key information and verifying the signature of the message by the receiver (page 509, Section 12.5.2, first paragraph). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Asanoma and Chen to sign the rekey request and verifying the corresponding signature, as taught by Menezes. The motivation for doing so would have been to provide source authentication (page 509, Section 12.5.2, first paragraph).

Allowable Subject Matter

18. Subject to the above 101 and 112, 2nd paragraph, rejections, claims 10 and 24 would be allowable over the prior art of record if rewritten to include all of the limitations of the base claim and any intervening claims.

19. The following is a statement of reasons for the indication of allowable subject matter. Regarding claim 10, the limitation "reading a key identifier of the private key; comparing the read key identifier to key identifiers of

previously deleted private keys; and rejecting the key request if the read key identifier matches any of the key identifiers of previously deleted keys", in combination with elements of the parent claims, have not been taught by prior art. Claim 24 is an apparatus claim corresponding to claim 10.

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 5,680,458 to Spelman et al.

U.S. Patent No. 6,240,187 to Lewis

U.S. Patent No. 6,978,017 to Wiener et al.

U.S. Patent No. 7,206,936 to Aull et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MD/
Minh Dinh
Examiner
Art Unit 2132

6/25/07

Benjamin G. Lanier
Examiner AU 2132